

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-332742

(P2000-332742A)

(43) 公開日 平成12年11月30日 (2000. 11. 30)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 D 0 4 4
			3 2 0 B 5 J 1 0 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 9 A 0 0 1
G 1 1 B 20/10		G 1 1 B 20/10	H

審査請求 未請求 請求項の数 4 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願平11-136695

(22) 出願日 平成11年5月18日 (1999. 5. 18)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 濱田 一郎

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 藤井 麻子

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

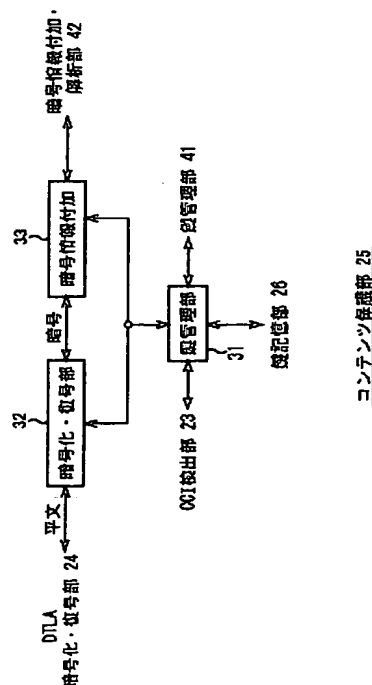
最終頁に続く

(54) 【発明の名称】 宿報処理装置および方法、並びに提供媒体

(57) 【要約】

【課題】 コンテンツの不正利用を抑止する。

【解決手段】 鍵管理部31は、アプリケーションが有する認証鍵K_nが正規のものであるかを判定し、正規のものであると判定したときだけ、アプリケーションとのコンテンツの授受を実行するように、コンテンツ保護部25を制御する。暗号化・復号部32は、復号されているコンテンツを、鍵管理部31から入力される暗号鍵K_cを用いて暗号化し、暗号情報付加部33に出力する。暗号情報付加部33は、暗号化・復号部32からの暗号化されたコンテンツに、暗号情報を付加して、アプリケーションに出力する。



【特許請求の範囲】

【請求項1】 著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置において、

入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成手段と、

前記暗号鍵を用いて前記コンテンツを暗号化する暗号化手段と、

前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定手段と、

前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成手段と、

前記秘密鍵生成手段が生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化手段により暗号化された前記コンテンツを、前記判定手段の判定結果に対応して、前記アプリケーションプログラムに供給する供給手段とを含むことを特徴とする情報処理装置。

【請求項2】 前記判定手段は、リボケーションリストを参照することにより前記認証鍵の正当性を判定することを特徴とする請求項1に記載の情報処理装置。

【請求項3】 著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置の情報処理方法において、

入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、

前記暗号鍵を用いて前記コンテンツを暗号化する暗号化ステップと、

前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定ステップと、

前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、

前記秘密鍵生成ステップで生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化ステップで暗号化した前記コンテンツを、前記判定ステップの判定結果に対応して、前記アプリケーションプログラムに供給する供給ステップとを含むことを特徴とする情報処理方法。

【請求項4】 著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置に、

入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、

前記暗号鍵を用いて前記コンテンツを暗号化する暗号化ステップと、

前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定ステップと、

前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、

前記秘密鍵生成ステップで生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化ステップで暗号化した前記コンテンツを、前記判定ステップの判定結果に対応して、前記アプリケーションプログラムに供給する供給ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、コンテンツの不正利用を抑止する場合に用いて好適な情報処理装置および方法、並びに提供媒体に関する。

【0002】

【従来の技術】 従来、著作権が保護されているコンテンツ（例えば、CD(Compact Disc)に記録されているオーディオデータ、DVD(Digital Versatile Disc)に記録されているAVデータ等）が不正に複製されることを抑止するために、コンテンツを記録可能な装置（例えば、MD(Mini Disc)レコーダ、CD-Rレコーダ、DV(Digital Video)レコーダ等）には、SCMS(Serial Copy Management System)、またはCGMS(Copy Generation Management System)が採用されている。SCMSやCGMSにおいては、コンテンツに所定の情報を付加し、その情報に基づいてコピー可能な回数を制限している。

【0003】 また、最近、コンテンツを再生、または記録するAV装置とパーソナルコンピュータとの間で、IEEE 1394バスを介してコンテンツを通信することが可能となった。さらに、パーソナルコンピュータにおいては、CPU(Central Processing Unit)の高速化やハードディスクの大容量化にともない、上述したコンテンツを再生し、記録し、さらに編集することが可能となった。

【0004】

【発明が解決しようとする課題】 したがって、パーソナルコンピュータに、上述したコンテンツに付加されている情報を意図的に改ざんするような不正なアプリケーションプログラムがインストールされている場合、コンテンツが違法にコピーされてしまうことを抑止できない課題があった。

【0005】 本発明はこのような状況に鑑みてなされたものであり、パーソナルコンピュータにおいて、アプリケーションプログラムに供給される直前のコンテンツを暗号化することにより、不正なアプリケーションプログ

ラムを用いたコンテンツの不正利用を抑止できるようにするものである。

【0006】

【課題を解決するための手段】請求項1に記載の情報処理装置は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成手段と、暗号鍵を用いてコンテンツを暗号化する暗号化手段と、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定手段と、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成手段と、秘密鍵生成手段が生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化手段により暗号化されたコンテンツを、判定手段の判定結果に対応して、アプリケーションプログラムに供給する供給手段とを含むことを特徴とする。

【0007】請求項3に記載の情報処理方法は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、暗号鍵を用いてコンテンツを暗号化する暗号化ステップと、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定ステップと、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、秘密鍵生成ステップで生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化ステップで暗号化したコンテンツを、判定ステップの判定結果に対応して、アプリケーションプログラムに供給する供給ステップとを含むことを特徴とする。

【0008】請求項4に記載の提供媒体は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、暗号鍵を用いてコンテンツを暗号化する暗号化ステップと、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定ステップと、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、秘密鍵生成ステップで生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化ステップで暗号化したコンテンツを、判定ステップの判定結果に対応して、アプリケーションプログラムに供給する供給ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0009】請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体においては、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵が生成され、暗号鍵を用いてコンテンツが暗号化される。また、アプリケーションプログラムから入力される認証鍵を用

いて秘密鍵が生成されて、アプリケーションプログラムの正当性が判定され、その判定結果に対応して、秘密鍵を用いて暗号化した暗号鍵、および暗号化されているコンテンツが、アプリケーションプログラムに供給される。

【0010】

【発明の実施の形態】本発明を適用したパーソナルコンピュータの構成例について、図1を参照して説明する。このパーソナルコンピュータ(PC)1は、IEEE1394バス2を介して、コンテンツを扱うことが可能な機器（例えば、図1に示すようなDVレコーダ(DVR)3、セットトップボックス(STB)4、およびハードディスク(HDD)5等）と接続されている。なお、IEEE1394バス2を介して通信されるコンテンツは、CPTWG(CopyProtection Technical Working Group)で推奨されるライセンス管理会社DTLA(Digital Transmission Licensing Administrator)がライセンスする方式（以下、DTLA方式と記述する）に基づいて暗号化されている。

【0011】パーソナルコンピュータ1は、バス16を介して接続されている、IEEE1394インタフェース11、CPU12、RAM13、ROM14、およびハードディスク15から構成される。IEEE1394インタフェース11は、IEEE1394バス2を介して、他の機器(DVR3等)から入力されるコンテンツを、パーソナルコンピュータ1で起動されている、コンテンツに対して再生、記録、編集等が可能なアプリケーションプログラム（以下、起動されている、コンテンツに対して再生、記録、編集等が可能なアプリケーションプログラムを、単にアプリケーションと記述する）に供給する。また、IEEE1394インタフェース11は、アプリケーションが処理したコンテンツを、IEEE1394バス2を介して他の機器に出力する。

【0012】なお、アプリケーションプログラムは、ハードディスク15に記憶されており、ROM14に記憶されているBIOSに基づくCPU12の制御によって、RAM13に転送されて起動される。また、このアプリケーションプログラムに対しては、DTLAのような暗号システムの管理者から固有の認証鍵 K_n が与えられているが、この認証鍵 K_n を得るためには、アプリケーションプログラムの制作元、およびユーザが、著作権が保護されているコンテンツを不正に利用しない旨を契約書等で誓約する必要がある。また、本明細書においてシステムの用語は、複数の装置、手段などにより構成される全体的な装置を意味するものである。

【0013】ここで、認証鍵 K_n には、IDとSignatureの対となる2値が含まれており、一方に所定の演算式を適用した結果が他方となっている。また、双方に所定の演算式を適用することにより、正しい対であることが確認できる。この所定の演算式を知っている、すなわち、認証鍵 K_n の正当性を判定できるのは、鍵管理部31（図3）だけである。また、所定の演算式を、IDとSign

atureを用いた逆算により求めることは非常に困難であるので、事実上、認証鍵 K_n を偽造することは不可能である。

【0014】図2は、IEEE1394インタフェース11の詳細な構成例を示している。制御部21は、IEEE1394インタフェース11の各部を制御する。入出力部22は、IEEE1394バス2から入力される、DTLA方式で暗号化されているコンテンツを受け付けてCCI(Copy Control Information)検出部23に出力する。CCI検出部23は、入出力部22から入力されるコンテンツをDTLA暗号化・復号部24に供給するが、その際、コンテンツのヘッダに記録されているCCI(2ビット)を検出して、制御部21、DTLA暗号化・復号部24、およびコンテンツ保護部25に供給する。

【0015】なお、CCIは、自身が付加されているコンテンツに対して許可されているコピーの制御を示す情報であり、00、10、01、11の4種類の状態がある。CCIが00(Copy free)である場合、対応するコンテンツに対しては無制限回数のコピーが許可されていることを意味している。CCIの状態が10(One Generator Copy Possible)である場合、対応するコンテンツに対しては1回だけコピーが許可されていることを意味している。CCIの状態が01(No More Copy)である場合、対応するコンテンツは、CCIの状態が10であるコンテンツを複製したもの(2世代目)であって、これに対してはコピーが許可されていないことを意味している。CCIの状態が11(Never copy)である場合、対応するコンテンツに対してはコピーが許可されていないことを意味している。

【0016】DTLA暗号化・復号部24は、CCI検出部23から入力されたDTLA方式で暗号化されているコンテンツを復号し、コンテンツ保護部25に出力する。また、DTLA暗号化・復号部24は、コンテンツ保護部25から入力されるコンテンツを、DTLA方式の用いて暗号化して入出力部22に出力する。なお、DTLA暗号化・復号部24における暗号化および復号は、DTLA暗号化・復号部24とコンテンツを出力した装置(DVR3等)の間における、DTLA方式で定義されている相互認証作業が終了した後に行われる。

【0017】コンテンツ保護部25は、DTLA暗号化・復号部24から入力されるコンテンツを暗号化してアプリケーションに供給する。また、コンテンツ保護部25は、アプリケーションから入力される、暗号化されているコンテンツを復号してDTLA暗号化・復号部24に供給する。鍵記憶部26は、コンテンツ保護部25における暗号化処理に用いられるソース鍵 K_s を、CCIの状態毎に複数個記憶している。

【0018】図3は、コンテンツ保護部25の詳細な構成例を示している。鍵管理部31は、アプリケーションの鍵管理部41(図4)から入力される認証鍵 K_n が正

規のものであるかを判定し、認証鍵 K_n が正規のものであると判定したときだけ、アプリケーションとのコンテンツの授受を実行するように、コンテンツ保護部25の各部を制御する。

【0019】すなわち、鍵管理部31は、アプリケーションからの認証鍵 K_n に含まれるIDに所定の演算式を適用し、その結果が対応するSignatureと等しいか否かを判定し、演算結果がSignatureと等しい(認証鍵 K_n が正規のものである)と判定した場合、さらに、IDとSignatureに所定の演算式を適用することにより、正しい対であるか否かを判定し、正しい対であると判定した場合、CCI検出部23から入力されるCCIの状態に対応するソース鍵 K_s を読み出し、ソース鍵 K_s および乱数を用いて暗号鍵 K_c を生成して、暗号化・復号部32に供給する。なお、暗号鍵 K_c は、所定の周期(例えば、30秒間乃至120秒間)毎に更新される。また、鍵管理部31は、CCIの状態を、暗号鍵 K_c を更新する毎に暗号情報付加部33に出力する。さらに、鍵管理部31は、アプリケーションの鍵管理部41から入力される認証鍵等の秘密鍵 K_a 算出用情報に基づいて秘密鍵 K_a を生成し、暗号鍵 K_c を秘密鍵 K_a を用いて暗号化して鍵管理部41に出力する。

【0020】暗号化・復号部32は、DTLA暗号化・復号部24からの復号されているコンテンツを、鍵管理部31からの暗号鍵 K_c を用いて暗号化し、暗号情報付加部33に出力する。また、暗号化・復号部32は、暗号情報付加部33からの、暗号化されているコンテンツを復号してDTLA暗号化・復号部24に出力する。

【0021】暗号情報付加部33は、暗号化・復号部32からの暗号化されたコンテンツに、CCIの状態(2ビット)、暗号鍵 K_c が更新される毎に切り替えられるevenまたはodd(1ビット)の暗号情報を付加して、アプリケーションの暗号情報解析部42(図4)に出力する。また、暗号情報付加部33は、暗号情報解析部42からの暗号化されたコンテンツを、暗号化・復号部32に出力する。

【0022】図4は、コンテンツに対し再生、記録、編集等が可能なアプリケーションの機能ブロック図を示している。鍵管理部41は、アプリケーションプログラムに対して与えられている認証鍵 K_n を記憶しており、アプリケーションがコンテンツの授受を開始する前に、記憶している認証鍵 K_n を、秘密鍵 K_a 算出用情報とともに、コンテンツ保護部25の鍵管理部31に出力する。また、鍵管理部41は、暗号情報解析部42から入力される、暗号情報に含まれる暗号鍵 K_c の更新を示す情報(evenまたはodd)が切り替えられたか否かを示す情報に対応して、鍵管理部31からの秘密鍵 K_a で暗号化されている暗号鍵 K_c を復号し、暗号化・復号部43に出力する。

【0023】暗号情報解析部42は、暗号情報付加部3

3から入力される、暗号鍵Kcで暗号化されているコンテンツを暗号化・復号部43に出力し、付加されている暗号情報を鍵管理部41に出力する。また、暗号情報解析部42は、暗号化・復号部43からの暗号化されたコンテンツを暗号情報付加部33に出力する。

【0024】暗号化・復号部43は、暗号情報解析部42からの入力される暗号鍵Kcで暗号化されているコンテンツを、鍵管理部41からの暗号鍵Kcを用いて復号し、コンテンツ処理部44に出力する。また、暗号化・復号部43は、コンテンツ処理部44から入力されるコンテンツを暗号化し、暗号情報解析部42に出力する。

【0025】コンテンツ処理部44は、入力されたコンテンツに対して、ユーザの操作に対応する処理（再生、記録、または編集等）を実行する。なお、コンテンツ処理部44には、暗号情報解析部42が解析した暗号情報に含まれるCCIが供給されるので、コンテンツ処理部44においては、CCIに反するような処理（制限回数を超えるコピー等）は実行されない。

【0026】なお、IEEE1394インタフェース11を1個のLSI(Large Scale Integrated circuit)で実現すれば、回路の途中から復号されたコンテンツを読み出すような不正行為を抑止することが可能となる。

【0027】次に、アプリケーションにコンテンツを入力する処理について、図5のフローチャートを参照して説明する。この入力処理は、IEEE1394インタフェース11にDTLA方式で暗号化されているコンテンツが入力され、そのCCIが、CCI検出部23で検出されてコンテンツ保護部25の鍵管理部31に入力され、DTLA方式で暗号化されているコンテンツが、DTLA暗号化・復号部24で復号されてコンテンツ保護部25の暗号化・復号部32に入力された後に実行される。

【0028】ステップS1において、アプリケーションの鍵管理部41は、コンテンツ入力の要求、記憶している認証鍵Kn、および秘密鍵Ka算出用情報を出力し、それらを、コンテンツ保護部25の鍵管理部31が受け付ける。

【0029】ステップS2において、鍵管理部31は、鍵管理部41からの認証鍵Knが正規のものであるかを判定し、認証鍵Knが正規のものであると判定した場合、ステップS3に進む。

【0030】ステップS3において、鍵管理部31は、CCIのステートに対応するソース鍵Ksを鍵記憶部26から読み出して、ソース鍵Ksと乱数を用いて暗号鍵Kcを生成し、暗号化・復号部32に出力する。また、鍵管理部31は、暗号鍵Kcを更新するタイミングを計測するタイマを0にリセットする。

【0031】ステップS4において、鍵管理部31は、秘密鍵Ka算出用情報を用いて秘密鍵Kaを生成し、さらに、秘密鍵Kaを用いて暗号鍵Kcを暗号化し、アプリケーションの鍵管理部41に出力する。鍵管理部41

は、暗号鍵Kcを復号する。

【0032】ステップS5において、暗号化・復号部32は、DTLA暗号化・復号部24からの復号されているコンテンツを、鍵管理部31からの暗号鍵Kcを用いて暗号化し、暗号情報付加部33に出力する。

【0033】ステップS6において、暗号情報付加部33は、CCIのステート、暗号鍵Kcの更新を示す情報（いまの場合、暗号鍵Kcは更新されていないのでeven）から成る暗号情報を生成し、暗号化・復号部32からの暗号化されたコンテンツに付加して、アプリケーションの暗号情報解析部42に出力する。暗号情報解析部42は、暗号情報に含まれる、暗号鍵Kcの更新を示す情報が切り替えられているか否かを判定し、判定結果を鍵管理部41に出力する。鍵管理部41は、この判定結果に基づき、いまの暗号鍵Kcを暗号化・復号部43に供給する。暗号化・復号部43は、暗号鍵Kcを用いてコンテンツを復号し、コンテンツ処理部44に出力する。

【0034】ステップS7において、鍵管理部31は、全てのコンテンツをコンテンツ保護部25からアプリケーションに出力したか否かを判定し、全てのコンテンツを出力していないと判定した場合、ステップS8に進む。ステップS8において、鍵管理部31は、自己のタイマを参照することにより、いまの暗号鍵Kcが用いられている時間を検知し、その時間が所定時間（30秒間乃至120秒間）を経過したか否かを判定する。いまの暗号鍵Kcが用いられている時間が所定時間を経過していないと判定された場合、ステップS5に戻り、それ以降の処理が繰り返される。

【0035】その後、ステップS8において、いまの暗号鍵Kcの使用時間が所定時間を経過したと判定された場合、ステップS9に進む。ステップS9において、鍵管理部31は、ソース鍵Ksと、再度発生させた乱数を用いて暗号鍵Kcを生成（更新）し、暗号化・復号部32に出力する。また、鍵管理部31は、自己のタイマを0にリセットする。

【0036】その後、ステップS4に戻り、ステップS7で全てのコンテンツを出力したと判定されるまで、以降の処理が繰り返される。ただし、ステップS6で付加される暗号情報に含まれる、暗号鍵Kcの更新を示す情報は、ステップS9で暗号鍵Kcが更新されているのでevenからoddに切り替えられる。この暗号鍵Kcの更新を示す情報に対応して、鍵管理部41から暗号化・復号部32に供給される暗号鍵Kcも更新される。

【0037】なお、ステップS2において、認証鍵Knが正規のものではないと判定された場合、ステップS10に進む。ステップS10において、鍵管理部31は、アプリケーションの鍵管理部41に対して、認証は不可能である旨を通知する。

【0038】次に、アプリケーションで処理されたコン

テンツをIEEE1394バス2に出力する処理について、図6のフローチャートを参照して説明する。この出力処理は、アプリケーションのコンテンツ処理部44において編集されたコンテンツが暗号化・復号部43に入力された後に実行される。

【0039】ステップS21において、アプリケーションの鍵管理部41は、コンテンツ出力の要求、記憶している認証鍵K_n、秘密鍵K_a算出用情報、および出力するコンテンツに対して設定するCCIのステートを、コンテンツ保護部25の鍵管理部31に出力する。

【0040】ステップS22において、鍵管理部31は、鍵管理部41からの認証鍵K_nが正規のものであるか否かを判定し、認証鍵K_nが正規のものであると判定した場合、ステップS23に進む。

【0041】ステップS23において、鍵管理部31は、鍵管理部41から入力されたCCIのステートに対応するソース鍵K_sを鍵記憶部26から読み出して、ソース鍵K_sと乱数を用いて暗号鍵K_cを生成し、暗号化・復号部32に供給する。ステップS24において、鍵管理部31は、鍵管理部41からの秘密鍵K_a算出用情報を用いて秘密鍵K_aを生成し、さらに、秘密鍵K_aを用いて、ステップS22で生成した暗号鍵K_cを暗号化し、アプリケーションの鍵管理部41に出力する。鍵管理部41は、暗号鍵K_cを復号して、暗号化・復号部43に出力する。

【0042】ステップS25において、アプリケーションの暗号化・復号部43は、鍵管理部41からの暗号鍵K_cを用いて、コンテンツ処理部44から入力されたコンテンツを暗号化し、暗号情報解析部42および暗号情報付加部33を介して、暗号化・復号部32に出力する。

【0043】ステップS26において、暗号化・復号部32は、ステップS23で鍵管理部31から入力された暗号鍵K_cを用いて、アプリケーション（暗号化・復号部43）からの暗号化されたコンテンツを復号し、DTLA暗号化・復号部24に出力する。

【0044】ステップS27において、DTLA暗号化・復号部24は、コンテンツ保護部25の暗号化・復号部32から入力された復号されているコンテンツを、DTLA方式で暗号化し、入出力部22に出力する。

【0045】ステップS28において、入出力部22は、DTLA暗号化・復号部24からのDTLA方式で暗号化されているコンテンツをIEEE1394バス2に出力する。

【0046】なお、ステップS2-2において、認証鍵K_nが正規のものではないと判定された場合、ステップS29に進む。ステップS29において、鍵管理部31は、アプリケーションの鍵管理部41に対して、認証は不可能である旨を通知する。

【0047】また、この出力処理においても、上述した入力処理と同様、周期的に暗号鍵K_cを変更するように

してもよい。

【0048】以上のように、本実施の形態によれば、正規の認証鍵K_nを持っているアプリケーションに対してだけ、IEEE1394インタフェース11のコンテンツ保護部25は、コンテンツの授受を行うようになされている。しかしながら、コンテンツの違法コピー等を実行可能なアプリケーションが、何らかの方法により、正規の認証鍵K_nを取得し、コンテンツが不正に利用されてしまうことも考えられる。そこで、本発明においては、認証鍵K_nの正当性を判定するコンテンツ保護部25の鍵管理部31に、不正に使用された認証鍵K_nが登録されているリボケーションリストを記憶させ、認証処理の際、鍵管理部31は、認証鍵K_nに含まれるIDとSignatureの整合性の判定に加えて、リボケーションリストとの照合を実行するようにして、リボケーションリストに登録されている認証鍵K_nは、IDとSignatureが対となっていてても正規なものであると判定されないようになされている。

【0049】なお、このリボケーションリストに関しては、その最新のものをインターネットやIEEE1394バス2等のネットワークを介して、鍵管理部31に配信する方法が考えられる。また、このリボケーションリストの利用方法としては、認証鍵K_nを個々に登録する方法と、複数の認証鍵K_nをまとめて登録する方法（例えば、認証鍵K_nのIDのMSB(Most Significant Bit)側の所定ビットを指定する等）が考えられる。複数の認証鍵K_nをまとめて登録する方法により、例えば、特定のソフトウェアメカ（認証鍵K_nを取得する際に誓約した規約に対する違反が発覚したソフトウェアメカ）が製作した全てのアプリケーションを、正規なものではないと判定させることが可能となる。

【0050】また、コンテンツ保護部25からアプリケーションへのコンテンツの出力を検知し、その回数をインターネット等を介して、コンテンツの著作権の所有者や暗号システムの管理者に通知するようにすれば、コンテンツや暗号システムを使用したことに対して、ユーザに課金することや、暗号システムの使用状況を把握することが可能となる。

【0051】なお、本発明は、IEEE1394バスに伝送されるコンテンツのアイソクロナスパケットおよびアシンクロナスパケット、並びに、他の伝送媒体に伝送されるコンテンツのパケットに対して適用することが可能である。

【0052】また、上記各処理を行うコンピュータプログラムは、磁気ディスク、CD-ROM等の情報記録媒体よりなる提供媒体のほか、インターネット、デジタル衛星などのネットワーク提供媒体を介してユーザに提供することができる。

【0053】

【発明の効果】以上のように、請求項1に記載の情報処

理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体によれば、認証鍵を用いてアプリケーションプログラムの正当性を判定し、その判定結果に対応して、秘密鍵を用いて暗号化した暗号鍵、および暗号鍵で暗号化されているコンテンツを、アプリケーションプログラムに供給するようにしたので、コンテンツの不正利用を抑止することが可能となる。

【図面の簡単な説明】

【図1】 本発明を適用したパーソナルコンピュータ1の構成例を示すブロック図である。

【図2】 図1のIEEE1394インタフェース11の構成例を示すブロック図である。

【図3】 図2のコンテンツ保護部25の構成例を示すブロック図である。

【図4】 パーソナルコンピュータ1で起動されているアプリケーションの機能を示すブロック図である。

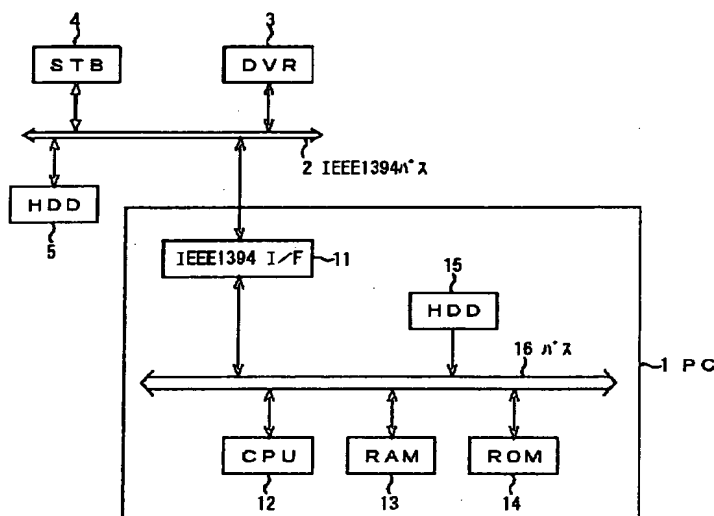
【図5】 図1のIEEE1394インタフェース11の動作を説明するフローチャートである。

【図6】 図1のIEEE1394インタフェース11の動作を説明するフローチャートである。

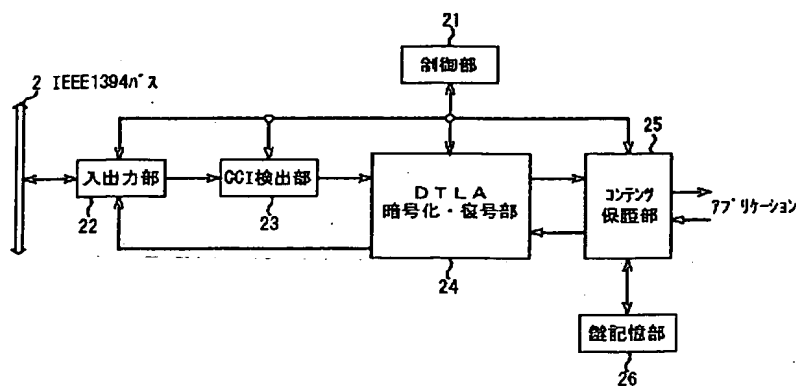
【符号の説明】

1 パーソナルコンピュータ, 2 IEEE1394バス, 11 IEEE1394インタフェース, 25 コンテンツ保護部, 31 鍵管理部, 32 暗号化・復号部, 33 暗号情報付加部, 41 鍵管理部, 42 暗号情報解析部, 43 暗号化・復号部, 44 コンテンツ処理部

【図1】

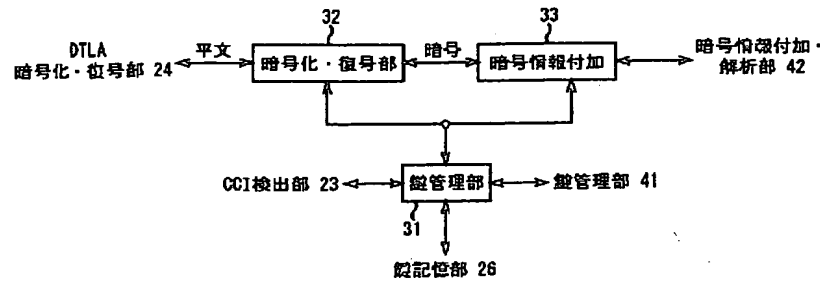


【図2】

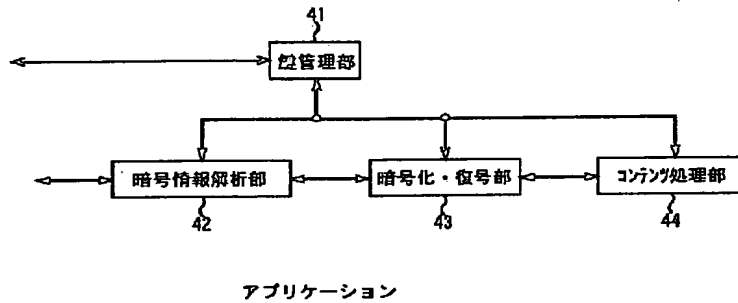


IEEE1394 I/F 11

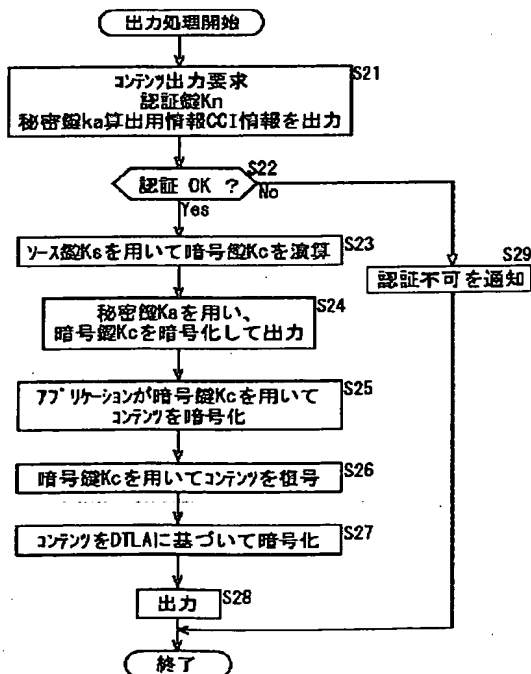
【図3】



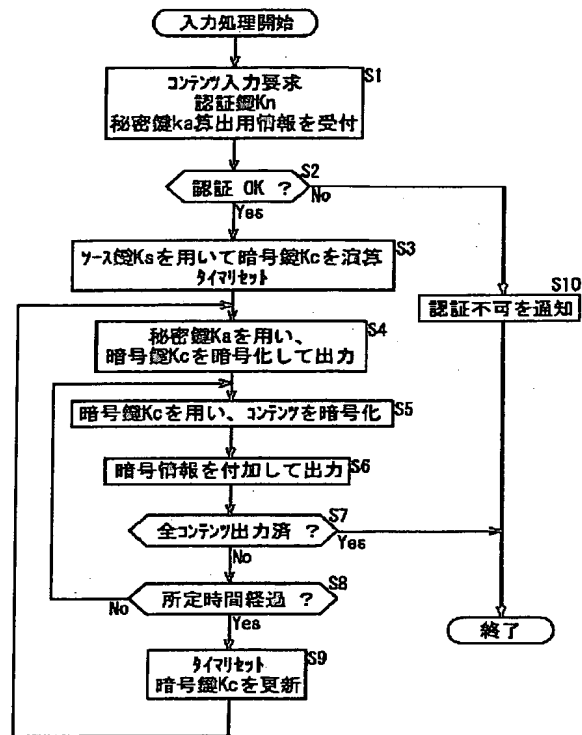
【図4】



【図6】



【図5】



フロントページの続き

(51) Int. Cl. 7

H04L 9/32

識別記号

F1

H04L 9/00

ターマコード (参考)

601E

673B

Fターム(参考) 5B017 AA06 BA05 BA07 BB02 BB03
 BB10 CA07 CA09 CA16
 5D044 BC01 CC04 DE17 GK17 HL01
 5J104 AA07 AA16 EA04 EA17 KA02
 MA02 NA02 NA32 PA14
 9A001 BB01 BB03 BB04 BB05 CC05
 DD06 EE03 GG22 JJ25 KK37
 LL03